BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L

A2

(11) International Publication Number: WO 00/08794

(43) International Publication Date: 17 February 2000 (17.02.00)

(21) International Application Number: PCT/US99/17786

(22) International Filing Date: 4 August 1999 (04.08.99)

(30) Priority Data:

09/129,467	4 August 1998 (04.08.98)	US
Not furnished	4 August 1999 (04.08.99)	US

(71)(72) Applicants and Inventors: SENATOR, Steven, T. [US/US]; 8625 Westminster Drive, Colorado Springs, CO 89020 (US). BLUMENTHAL, John [US/US]; 4432 East Emigration Canyon, Salt Lake City, UT 84018 (US). MULLIGAN, M., Geoff [US/US]; 2175 Cloverdale Drive, Colorado Springs, CO 80920 (US). FRASCADORE, Gregory, A. [US/US]; 9505 Morgan Road, Colorado Springs, CO 80908 (US).

(74) Agents: STRINGHAM, John, C. et al.; Workman, Nydegger & Seeley, 1000 Eagle Gate Tower, 60 East South Temple, Salt Lake City, UT 84111 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

Without international search report and to be republished upon receipt of that report.

(54) Title: SYSTEMS AND METHODS FOR SECURING ELECTRONIC MESSAGE

(57) Abstract

System and methods are provided for permitting a sender to control access to an electronic message. The sender selects one or more policies which are packaged with the electronic message to form an object. The policies are implemented as computer–executable instructions capable of execution on a remote computer. The recipient can only access the electronic message as dictated by the policies which are in the object. Unauthorized use of the electronic message is substantially prevented and the electronic message remains in the control of the sender.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

SYSTEMS AND METHODS FOR SECURING ELECTRONIC MESSAGE

BACKGROUND OF THE INVENTION

Related Applications

This application claims the benefit of U.S. Application No. 09/129,467, filed August 4, 1998, which is incorporated herein by reference.

The Field of the Invention

The present invention relates to electronic messaging. More particularly, the present invention relates to rendering electronic messages in a controlled manner.

The Prior State of the Art

Electronic mail, or email, is a type of electronic message that involves the transmission of messages over a communications network, which can be the internet, a local area network (LAN), a wide area network (WAN) or other network. In today's world, anyone with a computer can have access to email and email systems. Businesses have begun to rely on email as a method for interoffice communications and companies that are fully networked make extensive use of email because it is fast, flexible, and reliable.

Because the use of email has exploded in recent years, the capabilities and features of email systems and programs have also improved. For example, practically all email programs allow the user to attach files to a text message. The attachment may be a photo, a video clip, a sound byte, or other data. A user has the ability to send almost anything via email. A single email can be simultaneously sent to more than one person without having to retype the text of the message. An email can be stored on the recipient's computer as a text file, or be forwarded to a different user, or printed.

Email systems also have the ability to enhance the appearance of the text in the email. Users can select the color and font of the text in the email to enhance the visual appearance of the email. Other email applications notify a user when an email is received and opened by the recipient. Other additions to email systems include address books and scheduling applications. Address books allow a user to store email addresses and personal information about the recipient. In sum, Email applications are not only becoming sophisticated, but are also becoming indispensable.

Currently, there are two predominant types of email applications or systems: client based email and browser based email. Client based email involves a client side application stored on each client machine. The application typically provides, at a minimum, the tools necessary for a user to compose and send an email. A server receives the composed emails and forwards them to the recipients. Browser based email systems also provide the tools necessary for a user to compose an email, but each user or client machine does not have a separate application because the email application is accessible with an internet browser.

Many proprietary email systems provide additional tools which are not available to users outside of the local network. For instance, an email may be retractable by the sender within the proprietary system if the email has not yet reached the recipient. However, the additional tools are only available to clients served by that particular server,

or to families of that particular proprietary system. Browser based email and client based email systems do not have the ability to retract an email that has left the local mail server. Once an email has entered the internet, it will be received and read by the recipient. In some instances, the email may be read by unintended recipients. It would be advantageous to provide tools that function within any system.

Instant messaging is another example where an electronic message is sent to a recipient. Typically, a portal provides this service to users who are connected to the portal by having a user select or create a list of persons with whom instant messaging is desired. When a person on the list logs on to the portal, the creator of the list is notified. The creator can then send a message which is instantly received by the recipient. In many aspects, instant messaging is similar to a chat room where all users can view the messages of other users. Instant messaging, however, is typically limited to a known group of users which are all on a certain list.

Electronic messages can be sent in other methods. Currently, facsimile, printing and other services are available on the Internet. The common factor related to facsimiles, email, instant messaging and other services is data or information. The fundamental issue is that information has value and there is a need to protect that data as the use of electronic messages becomes more prominent in personal and business applications.

In many instances, the sender simply desires to maintain control over the information in the electronic message. Sending an electronic message can deprive the sender of that control. For example, many firms or businesses exist which search various publications and databases for a fee. These firms produce a report related to the search request of their clients. In many instances, the contents of the report can be sensitive. For example, the report may contain an analysis of whether a hostile corporate takeover is feasible. The report of these firms is valuable not only to the client, but also to the firm. With today's technology, the report may be sent to the client electronically. If the information in the report, however, is discovered by an unauthorized party, then damage has been done to both parties. In fact, many firms will not transmit sensitive data electronically for fear of the information being obtained by an unauthorized person.

Additionally, the information in an electronic message can be discovered either intentionally or inadvertently. For example, it is possible for a user to accidentally hit the forward button instead of the reply button in an email application. The result of this mistake is that the information may be addressed or delivered to the wrong person. In other instances, traffic on the Internet is monitored and intercepted to determine the content of the traffic. If sensitive information is sent, it is possible that the information will be intercepted and misused. The same perils exist with paper documents, but it is more complicated to copy a report and mail it to an unauthorized person than it is to simply click the forward button of an email application.

While electronic messages provide desirable advantages, there are corresponding disadvantages. Because information can be sent electronically and because the information is potentially discoverable by unauthorized individuals either inadvertently or intentionally, there is a need to protect the information, or minimize the risk that the data will be accessed without authorization. It would be an advance in the art to provide risk management to electronic messages.

OBJECTS AND SUMMARY OF THE INVENTION

It is therefore an object of one embodiment of the present invention to secure the contents of an electronic message.

It is another object of one embodiment of the present invention to provide risk management to electronic messages.

It is a further object of one embodiment of the present invention to prevent unauthorized use of electronic messages.

It is an additional object of one embodiment of the present invention to select policies for an electronic message.

It is yet another object of one embodiment of the present invention to integrate policies controlling access to an electronic message with the electronic message.

It is a further object of one embodiment of the present invention to create an electronic message with self-enforcing policies.

It is another object of one embodiment of the present invention to restrict access to electronic messages.

Risk management for electronic messages requires, in one embodiment, that access to electronic messages be monitored or restricted. This is difficult because once the electronic message has been sent to a recipient, it is no longer in the control of the sender. The present invention provides systems and methods for controlling the recipient's access to the electronic message.

In order for a sender to control access to an electronic message, the sender chooses policies which are to be enforced with respect to the electronic message. The policies are typically related to the use and access of the electronic message, but may serve other functions. For instance, a user may choose a policy which prevents a recipient from printing the electronic message or the user may choose a policy which prevents the electronic message from being forwarded to another user. Other functions include automatically forwarding the message to another user upon being opened by a recipient. In sum, policies can serve a wide variety of purposes for the sender.

After the policies have been selected by the sender, they are associated with the electronic message. The policies and the electronic message are then packaged together to form an object. The policies are represented, in one embodiment, by computer-executable instructions and are capable of executing on a remote machine. An example of such computer executable instructions is JAVA. This embodiment permits the object to enforce the policies selected by the sender on the recipient.

The present invention can be configured in a wide variety of ways. For instance, one embodiment uses a remote source to store the policies which the sender may associate with an electronic message. In this embodiment, the packaged object includes a Uniform Resource Identifier (URI) referring to a remote policy which must be accessed before access to the electronic message is granted to the recipient. The policies which may be stored at a remote location with respect to both the sender and the recipient, are enforced by the object.

In another embodiment, the policies may be coded instructions which represent policies which are stored on a remote location. The remote location may be referenced by a URI, or the remote location can be the recipient's computer or other rendering device. In other words, the recipient may have computer-executable instructions which can interpret the coded policies.

The present invention may be implemented in both client based systems as well as browser based systems. In environments that do not support the rendering of Hyper Text Markup Language (HTML) within the body of a received email, the object may arrive as an attachment. In one embodiment, the recipient is required to have a Java virtual machine before the policies integrated with the electronic message may be enforced.

Additional objects and advantages of the invention will be set forth in the description which follows, and in part will be obvious from the description, or may be learned by the practice of the invention. The objects and advantages of the invention may be realized and obtained by means of the instruments and combinations particularly pointed out in the appended claims. These and other objects and features of the present invention will become more fully apparent from the following description and appended claims, or may be learned by the practice of the invention as set forth hereinafter.

BRIEF DESCRIPTION OF THE DRAWINGS

In order that the manner in which the above-recited and other advantages and objects of the invention are obtained, a more particular description of the invention briefly described above will be rendered by reference to specific embodiments thereof which are illustrated in the appended drawings. Understanding that these drawings depict only typical embodiments of the invention and are not therefore to be considered limiting of its scope, the invention will be described and explained with additional specificity and detail through the use of the accompanying drawings in which:

Figure 1 is an exemplary system for implementing the present invention;

Figure 2 is a block diagram of an object comprising data packaged with one or more policies;

Figure 3 is a block diagram illustrating an exemplary method for creating a self-executing object; and

Figure 4 is a block diagram of a network implementing the systems and methods of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Electronic messages are used to convey information from one entity to another entity. As used herein, electronic message comprises email, instant messaging, facsimile, video files, audio files, graphics, text, documents, spreadsheets, databases and other data and information. A significant problem with electronic messages is that control of the electronic message passes from the sender to the recipient. In many instances, the sender desires to maintain control of the electronic message. This is true of confidential or sensitive information as well as of data that is copyrighted or otherwise protected by law.

Electronic messages provide a sender with the ability to quickly transmit information to a recipient, but as previously discussed, certain risks are involved. The protection a sender desires to impart to an electronic message can vary. Security, in any event, is never absolute. The present invention provides systems and methods for securing electronic messages from unauthorized use.

A sender, in a preferred embodiment of the present invention, creates or prepares an electronic message using either a client based or a browser based application. Policies are made available to the sender and the sender selects one or more of those policies to be associated with the electronic message. A packager is provided which packages the electronic message with the selected policies into an object. The policies associated with the message are capable of executing or of being executed at the recipient's computer or other rendering device and permit the sender of the electronic message to maintain control over the electronic message in the object. In effect, the use of the electronic message is dictated by the sender of the electronic message. In this manner, the risk of unauthorized use is reduced and the content of the electronic message is secured or protected.

The present invention is described in terms of diagrams and flow charts. Using the diagrams and flow charts in this manner to present the invention should not be construed as limiting its scope. The embodiments of the present invention may comprise a special purpose or general purpose computer comprising various computer hardware.

Embodiments within the scope of the present invention also include computer-readable media having computer-executable instructions or data structures stored thereon. Such computer-readable media can be any available media which can be accessed by a general purpose or special purpose computer. By way of example, and not limitation, such computer-readable media can comprise RAM, ROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to store the desired executable instructions or data structures and which can be accessed by a general purpose or special purpose computer. When information is transferred or provided over a network or other communication connection to a computer, the computer properly views the connection as a computer-readable medium. Thus, such a connection is also properly termed a computer-readable medium. Combinations of the above should also be included within the scope of computer-readable media. Computer-executable instructions comprise, for example, instructions and data which cause a general purpose computer, special purpose computer, or special purpose processing device to perform a certain function or group of functions. The computer-executable instructions and associated data structures represent an example of program code means for executing the steps of the invention disclosed herein.

Figure 1 and the following discussion are intended to provide a brief, general description of a suitable computing environment in which the invention may be implemented. Although not required, the invention will be described in the general context of computer-executable instructions, such as program modules, being executed by a personal computer. Generally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types. Moreover, those skilled in the art will appreciate that the invention may be practiced with other computer system configurations, including hand-held devices, multi-processor systems, microprocessor-based or programmable consumer electronics, network PCs, minicomputers, mainframe computers, and the like. The invention may also be practiced in distributed computing environments where tasks are performed by remote processing devices that are linked through a communications network. In a distributed computing environment, program modules may be located in both local and remote memory storage devices.

With reference to Figure 1, an exemplary system for implementing the invention includes a general purpose computing device in the form of a conventional computer 20, including a processing unit 21, a system memory 22, and a system bus 23 that couples various system components including the system memory to the processing unit. The system bus 23 may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures. The system memory includes read only memory (ROM) 24 and random access memory (RAM) 25. A basic input/output system (BIOS) 26, containing the basic routines that help to transfer information between elements within the computer 20, such as during start-up, may be stored in ROM 24. The computer 20 may also include a magnetic hard disk drive 27 for reading from and writing to a magnetic hard disk, not shown, a magnetic disk drive 28 for reading from or writing to a removable magnetic disk 29, and an optical disk drive 30 for reading from or writing to removable optical disk 31 such as a CD-ROM or other optical media. The magnetic hard disk drive 27, magnetic disk drive 28, and optical disk drive 30 are connected to the system bus 23 by a hard disk drive interface 32, a magnetic disk drive-interface 33, and an optical drive interface 34, respectively. The drives and their associated computer-readable media provide nonvolatile storage of computer readable instructions, data structures, program modules and other data for the computer 20. Although the exemplary environment described herein employs a magnetic hard disk 27, a removable magnetic disk 29 and a removable optical disk 31, it should be appreciated by those skilled in the art that other types of computer readable media which can store data that is accessible by a computer, such as magnetic cassettes, flash memory cards, digital video disks, Bernoulli cartridges, random access memories (RAMs), read only memories (ROM), and the like, may also be used in the exemplary operating environment.

A number of program modules may be stored on the hard disk, magnetic disk 29, optical disk 31, ROM 24 or RAM 25, including an operating system 35, one or more application programs 36, other program modules 37, and program data 38. A user may enter commands and information into the computer 20 through input devices such as a keyboard 40 and pointing device 42. Other input devices (not shown) may include a microphone, joy stick, game pad, satellite dish, scanner, or the like. These and other input devices are often connected to the processing unit 21 through a serial port interface 46 that is coupled to system bus 23, but may be connected by other interfaces, such as a parallel port, game port or a universal serial bus (USB). A monitor 47 or other type of display device is also connected to system bus 23 via an interface, such as video adapter 48. In addition to the monitor, personal computers typically include other peripheral output devices (not shown), such as speakers and printers.

The computer 20 may operate in a networked environment using logical connections to one or more remote computers, such as a remote computer 49. Remote computer 49 may be another personal computer, a server, a router, a network PC, a peer device or other common network node, and typically includes many or all of the elements described above relative to the computer 20, although only a memory storage device 50 has been illustrated in Figure 1. The logical connections depicted in Figure 1 include a local area network (LAN) 51 and a wide area network (WAN) 52 that are presented here by way of example and not limitation. Such networking environments are commonplace in offices enterprise-wide computer networks, intranets and the Internet.

When used in a LAN networking environment, the computer 20 is connected to the local network 51 through a network interface or adapter 53. When used in a WAN networking environment, the computer 20 typically includes a modem 54 or other means for establishing communications over the wide area network 52, such as the Internet. Additionally, computer networks may comprise wireless networks. The modem 54, which may be internal or external, is connected to the system bus 23 via the serial port interface 46. In a networked environment, program modules depicted relative to the computer 20, or portions thereof, may be stored in the remote memory storage device. It will be appreciated that the network connections shown are exemplary and other means of establishing a communications link between the computers may be used.

Figure 2 is a block diagram conceptually illustrating data to which access is restricted by policies. Electronic message 204 can be an email, an instant message, a video clip, an audio file, a document, a file, a Universal Resource Identifier (URI) or any other type of data which is to be protected. Polices 202 are intended to define how electronic message 204 can be used or accessed. Policies 202 and electronic message 204 are coupled or packaged together to form object 200.

Policies 202 are an important aspect of object 200 because policies 202 define, in one embodiment: the method of revealing or rendering electronic message 204; how electronic message 204 is to be accessed; and the ways in which a user may interact with or use electronic message 204. Exemplary polices, which may be selected by a sender of electronic message 204, include but are not limited to: indicating whether the recipient is permitted to forward electronic message 204 to another user; indicating whether a recipient is permitted to copy, paste or cut the content of electronic message 204; indicating whether a recipient is permitted to save electronic message 204 separate from policies 202; indicating whether a sender is able to retract electronic message 204 that has been sent or forwarded to the recipient or another user; and indicating whether a user can print electronic message 204. Other policies 202 may specify and/or include:

a date before which an electronic message may not be used, or a date after which an electronic message may no longer be used, or a time window in which the electronic message may be accessed;

the number of times an electronic message may be opened or accessed;

an audit trail, in which data pertaining to the usage history of an electronic message is captured and stored in a file or sent to another party, which may be the sender of the electronic message;

acceptance conditions or the presentation of acceptance conditions, which the recipient must accept before the electronic message is accessed or

opened, and the recording of the recipient's acceptance or rejection of the acceptance conditions as well as notification to a party, such as the sender, that the acceptance conditions have been accepted or rejected;

the number of times an electronic message may be accessed, opened or read, which may be once;

that a record of the use of the electronic message by the recipient may be created and sent or forwarded to another party which may be the sender;

that only a specific number or a larger number of electronic messages may be accessed or opened;

that only the first N number of copies of an electronic message may be opened or accessed;

that the receiver must choose a password or a pass phrase, which will be required for subsequent attempts to open the electronic message;

that only one copy of the electronic message is ever accessible or readable. and that the determination of which copy of the electronic message may be opened may depend on which copy is opened first, last, or by other conditions;

that messages require another condition to occur and that the conditions may be provided by an external source;

authorization via public key systems, symmetric key systems, passphrases. biometric characteristics, company badges, smart cards, JavaRings. or other forms of personal or group authorization;

that electronic messages are only accessible or readable in a specified order by particular recipients as in a routing slip;

that an electronic message cannot be captured by a printscreen function or other memory capturing method; and

that messages are only readable or accessible under specific environmental conditions, such as the time of day, the location of the attempt to access the electronic message, when another person is logged in and viewing the audit logs, etc.

Other polices can be implemented and all polices can be combined in complex relations.

Clearly, many policies can be implemented and enforced with respect to an electronic message.

In another embodiment, policies 202 may comprise a URI reference. The URI reference, which may be remotely located with respect to both the sender and recipient of the electronic message may contain the actual polices that the sender desires to enforce. In this instance, the policy packaged in the object would be the requirement to look to a remote source or location for additional policies which may affect the recipient's access to the electronic message.

Figure 3 is illustrative of the method by which object 200 is formed. Electronic message 204 is gathered or created by a user. For instance, a user may create an email which is to be sent to a recipient. The email, in this case, would be electronic message 204. After electronic message 204 has been created, associator 222 associates policies 202, which have been selected by the sender, with electronic message 204. At associator 222, policies 222 which are linked or associated with electronic message 204 and are not yet enforceable.

After electronic message 204 and policies 202 are associated, packager 220 packages them to create object 200. In one embodiment, this is done by creating a JAVA applet which is capable of executing on any recipient having a Java virtual machine. In other words, policies 202, in one embodiment, are computer-executable instructions that are capable of executing on a remote computer. In another embodiment, the policies packaged with an electronic message are coded instructions which invoke computer-executable instructions which reside in a separate or remote environment or location. For example, the local network of the recipient may have the computer-executable instructions necessary to execute the coded instructions stored on a server which is accessible by the recipient, or the computer of the recipient may contain the necessary computer-executable instructions, or the computer-executable instructions referenced by the coded instructions may reside on a remote location or environment. In other words, the policies packaged in an object can be executed and enforced in a variety of methods.

Once object 200 is formed, policies 202 are active and will control the recipient's access and use of electronic message 204. In this manner, object 200 is self-enforcing. In systems having a form of electronic messaging, such as email, the sender is no longer in physical control of the electronic message after it has been sent. Creating an object, which comprises data and computer-executable instructions, permits the sender of the data to ensure that the data is used appropriately by the recipient.

In addition to packaging data 202 with policies 204, packager 220, or associator 222 has the capability to encrypt electronic message 204. The encryption of data 202, in one embodiment, is to ensure that only the intended recipient has the capability of decrypting data 202. For example, if electronic message 204 is encrypted with a key that only a particular recipient possesses, forwarding data 202 to another user, while possible, is essentially useless because the data remains encrypted. The encryption is typically performed using methods well known in the art. In another embodiment, the encryption is to ensure that only when the conditions specified in the policies are satisfied can the message be decrypted and viewed.

Figure 4 is a block diagram of an exemplary system in which electronic messages may be sent. Network 230 is illustrated having a plurality of senders 232, packager 220, server 234 and path 236. Senders 232 are intended to be representative of the source of an electronic message or other data. In a preferred embodiment, sender 232 is a computer as described in Figure 1 which has the capability of creating and sending or transmitting an electronic message. Server 234 may also be embodied as a computer having the capability of sending or forwarding electronic messages created by sender 232. Server 234, in a preferred embodiment is a mail server or a web server. Packager 220, as described previously, creates object 200.

Packager 220 may also be embodied as a computer and is located, in a preferred embodiment, in the network such that all electronic messages are examined

or monitored by packager 220. Those electronic messages that have been associated with policies are manipulated by packager 220 to form object 200. Electronic messages that are not associated with policies are typically ignored by packager 220.

Server 234, upon receiving an electronic message, forwards or sends the electronic message to recipient 242. Typically, sender 232 and recipient 242 are connected via a network. In figure 4, Internet 238 is the connecting network. The electronic message, or object arrives at server 240 at which point recipient 242 is notified that an electronic message has arrived. Figure 4 illustrates that electronic messages or objects are sent and received in well known methods with the difference that packager 220 creates an object which is self-enforcing. In other words, the policies of the sent object define what recipient 242 can do with the electronic message in the object, rather than the particular application of the user.

Recipient 242, upon receiving the object, will only be able to access the data in the object as determined by the policies. In some embodiments, the policies are part of the object. In other embodiments, the policies may refer to a remote location which is independent of sender 232. For instance, source 244, which may be referenced by a URI, may contain the policies which are to be enforced against recipient 242. The object received by recipient 242, in this example, would cause source 244 to be accessed to determine the policies to be enforced against recipient 242.

Path 236 is representative of the path of the electronic message from sender 232 to packager 220. While the electronic message is in path 236, an object has not been formed and the electronic message is potentially discoverable by unauthorized persons. To protect against this possibility, a cryptographically secure connection may be employed for the transport of the electronic message.

In another embodiment, path 236 first leads to an associator, shown in Figure 3, which is located between sender 232 and packager 220. The associator typically performs a function separate from the function of the packager, but the associator is capable of performing its function at sender 232, at packager 220, or at some point in path 236. In another embodiment, the associator is integrated with sender 232 and in yet another embodiment, the associator is integrated with packager 220, and in another embodiment, the associator is separate from both sender 232 and packager 220 as illustrated in Figure 3. If the associator is executed on the same machine or computer as the environment in which an electronic message is created, path 236 is obviated.

Policy Selection

Policies are typically selected by the sender of an electronic message, although it is possible for an entity such as a corporation to automatically associate policies with each outgoing electronic message. There are at least two different environments from which a user may select policies. The first environment is a client based environment and the second environment is a browser-based environment.

In a client based environment, each client typically has a separate application which provides the user with the ability to create and transmit electronic messages. The messages are received by a mail server which transmits them to the recipient. In order for a user to select a policy, a module is integrated with the application which permits the user to select and associate policies with an electronic message. In one

embodiment, this is done by installing the module into each separate application for each sender. When a user or sender is creating an electronic message, the module permits the sender to select policies which will be associated with the electronic message or data to be sent. Later, the packager creates an object which comprises the code necessary to enforce the selected polices on the electronic message or data.

In a browser based environment, the application is typically located on a server computer and each user accesses the application using a browser. In one embodiment, the policies are made available to the user by altering options exposed to the user via the web pages which make up the user interface. A user can select the desired policies by simply pointing and clicking. The selected policies are then associated with the electronic message or data and the packager creates an object which has the capability of enforcing those policies.

In both environments, the user selects which polices are to be enforced on the electronic message. The module of the client based environment can be enlarged to include other polices or policies can be removed from an application. In a similar manner, the policies provided in the browser based environment can be removed or expanded. The policies can be adapted to each environment quickly and easily. A small install is usually required by the client based applications and the HTML code of the browser based services is easily altered at the server such that all users have access to policies. The selection of policies available to end users or senders may be determined by the original installation or modification previously mentioned. It may also be determined by a policy selection and configuration environment intended for management by a systems administrator.

Policies

The policies which may be selected by a user are usually intended to protect the electronic message or data of the user. For instance, the data may be a balance sheet of a corporation which is only intended to be viewed by a certain accountant. In other instances the data is copyrighted and is being sent electronically to the purchaser. In the case of emails, it is very simple for a recipient to forward an email to one or more persons. However, it is possible that this is not the intent of the sender. Policies are intended to protect against this and other situations where the data or electronic message is to be protected. The protection provided is not absolute in some instances, but the risk that the data will be used in an unauthorized manner is usually reduced.

A first policy is that of preventing a recipient from forwarding the electronic message to a new user and the policy can be enforced in a variety of methods. In the first method, the electronic method is encrypted with the public key of the recipient. Presumably, only the recipient has the private key, which is necessary to decrypt the message. If the electronic message is forwarded, it is forwarded in an encrypted form which the next user cannot decrypt because they do not possess the private key of the original recipient. Another method requires the sender and the recipient to agree to a password in a separate transaction, such as a telephone call, before the electronic message is sent to the recipient. The policies associated and integrated with the electronic message will require the recipient to supply a password before access is granted to the electronic message. If the electronic message is forwarded to another user, the policies will prevent the electronic message from being accessed because the new user presumably does not know the password. A final exemplary method of preventing an electronic message from being forwarded is to prevent the recipient

from being able to access the forwarding mechanism of the application. In some instances, this can be done by hiding the forward button of the recipient's electronic messaging application. Depending on the amount of security desired, a different mechanism can be employed for preventing a recipient from forwarding an electronic message. Combinations of the above mentioned methods are also possible. Each of the embodiments described for preventing unauthorized forwarding offers a different amount of security to the sender of the electronic message. In some instances, the intent of the sender may be to simply complicate the process. For example, an expert computer user may be able to forward an electronic message in the case where the forward button is hidden. The typical user, however, will be unable to forward the electronic message.

Another policy which may be selected by the user is the ability to cause an electronic message to expire. This policy can also be implemented in a variety of methods. In one method, the packager, which may be accessible by a URI, stores a date or time which indicates the expiration date of an object. When a recipient attempts to access the object, the policy of the objects checks the current date or time against the date or time stored at the packager. If the electronic message or object has expired, then access is denied to the recipient. In this embodiment, the data is frequently encrypted as an additional precaution. The source of the current date or time may be the clock on the recipient's computer, an external trusted time source, or a combination of such time sources.

Another embodiment is to store the expiration date at a remote location, which is also accessible using a URI. The object, before allowing the recipient access, checks the expiration time at the remote location, rather than the packager, to determine if the electronic message has expired. Clearly, these methods offer scaled security.

Another policy is the ability to retract an electronic message that has already been sent to a recipient. In one embodiment, the sender can register with the packager to indicate that the electronic message is to be retracted. The object which was sent to the recipient first checks with the packager to determine if the sender desires to retract the object. If the sender has indicated that the object is to be retracted, the policies of the object do not permit the recipient to access the data stored in the object. In this embodiment, the data may be encrypted as a further precaution. The operation of this policy is similar to the expiration policy.

Another policy which may be selected by the user is restricting the ability of the recipient to cut, copy or paste the contents of the object. When the recipient selects text to be cut or copied, the text is placed in a buffer or memory. In one embodiment, the policy of the object detects when text of the data in the object has been selected and placed in the buffer. The policy may either replace the data in the buffer with unrelated digital data or may simply cause the buffer to be emptied. In this manner, the recipient is prevented from cutting, copying and pasting the contents or text of the electronic message in the object.

The policies described above are intended to be exemplary of the type of policies which may be selected by the sender of an electronic message and are not intended to be limiting. The policies which may be made available to a sender can be altered or removed. Additional policies can be made available for the use of the sender and the policies can be enforced in a variety of methods. In some instances, the purpose of the policies is related to risk management of the data rather than

absolute security. However, the level of risk to the data can be varied as determined by the policy and the strength of the policy selected. An electronic message can be associated with more than one policy and in some instances, the policies to be enforced can be located in a remote location. The policies can be enforced in both client based and browser based environments.

The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

What is claimed and desired to be secured by United States Letters Patent is:

1. A method for creating a self enforcing object, the method comprising the steps of:

creating, by a sender, an electronic message;

associating one or more policies with the electronic message; and

packaging the electronic message with the one or more policies to form the self enforcing object.

2. A method as defined in claim 1, wherein the electronic message comprises an email.

3. A method as defined in claim 1, wherein the electronic message comprises an instant message.

4. A method as defined in claim 1, wherein the step of associating one or more policies with the electronic message further comprises the step of selecting, by the user, one or more policies.

5. A method as defined in claim 1, further comprising the step of encrypting the electronic message.

6. A method as defined in claim 1, wherein the one or more policies comprise computer-executable code.

7. A method as defined in claim 1, wherein the one or more policies comprise coded instructions which invoke computer-executable code which reside in a remote environment.

8. A method as defined in claim 1, wherein the policies control access to the electronic message.

9. A method as defined in claim 1, wherein the policies render the electronic message to a recipient of the electronic message.

10. A computer-readable medium having computer-readable instructions for performing the steps recited in claim 1.

11. A method for rendering an object having an electronic message at a recipient, the method comprising the steps of:

receiving the object at the recipient;

executing one or more policies packaged in the object with the electronic message; and

rendering, to the recipient, the electronic message according to the one or more policies.

12. A method as defined in claim 11, wherein the one or more policies comprise computer-executable code capable of executing on more than one computer.

13. A method as defined in claim 11, wherein the one or more policies comprise coded instructions which invoke computer-executable instructions which reside in a separate environment.

14. A method as defined in claim 11, wherein the one or more policies control access to the electronic message.

15. A method as defined in claim 11, wherein the step of rendering the electronic message further comprises the step of decrypting the electronic message.

16. A method as defined in claim 11, wherein the one or more policies prevents the electronic message from being forwarded.

17. A method as defined in claim 11, wherein the one or more policies enables a sender to retract an electronic message.

18. A method as defined in claim 11, wherein the one or more policies prevents an electronic message from being cut.

19. A method as defined in claim 11, wherein the one or more policies prevents an electronic message from being copied.

20. A method as defined in claim 11, wherein the one or more policies prevents an electronic message from being opened.

21. A method as defined in claim 11, wherein the one or more policies determines if the electronic message has expired.

22. A method as defined in claim 11, wherein the one or more policies prevents an electronic message from being printed.

23. A method as defined in claim 11, wherein the one or more policies prevents the electronic message being displayed on a display device from being captured via a printscreen function.

24. A method as defined in claim 11, wherein the one or more policies comprises a URI.

25. A computer-readable medium having computer-executable instructions for performing the steps recited in claim 11.

26. A method for controlling access by a recipient to an electronic message, the method comprising the steps of:

associating the electronic message with one or more policies;

packaging the one or more policies with the electronic message to form an object;

sending the object to the recipient; and

executing, at the recipient, the policies packaged with the electronic message.

27. A method as defined in claim 26, wherein the step of associating the electronic message further comprises the step of creating the electronic message.

28. A method as defined in claim 26, wherein the step of associating the electronic message further comprises the step of encrypting the electronic message.

29. A method as defined in claim 26, wherein the step of associating the electronic message further comprises the step of encrypting the one or more policies associated with the electronic message.

30. A method as defined in claim 26, wherein the step of associating the electronic message further comprises the step of selecting the one or more policies from a group of policies comprising:

a first policy for controlling whether the electronic message may be forwarded;

a second policy for controlling when the electronic message expires;

a third policy for retracting the electronic message;

a fourth policy for opening the electronic message;

a fifth policy for preventing the recipient from cutting the electronic message; and

a sixth policy for preventing the recipient from copying the electronic message.

31. A method as defined in claim 26, wherein the one or more policies comprise computer-executable instructions.

32. A method as defined in claim 26, wherein the one or more polices comprise coded instructions which invoke computer-executable code which reside in a separate environment.

33. A computer-readable medium having computer-executable instructions for performing the steps recited in claim 26.

34. A method for packaging an electronic message with one or more policies, the method comprising the steps of:

monitoring a network for electronic messages associated with one or more policies sent by a sender;

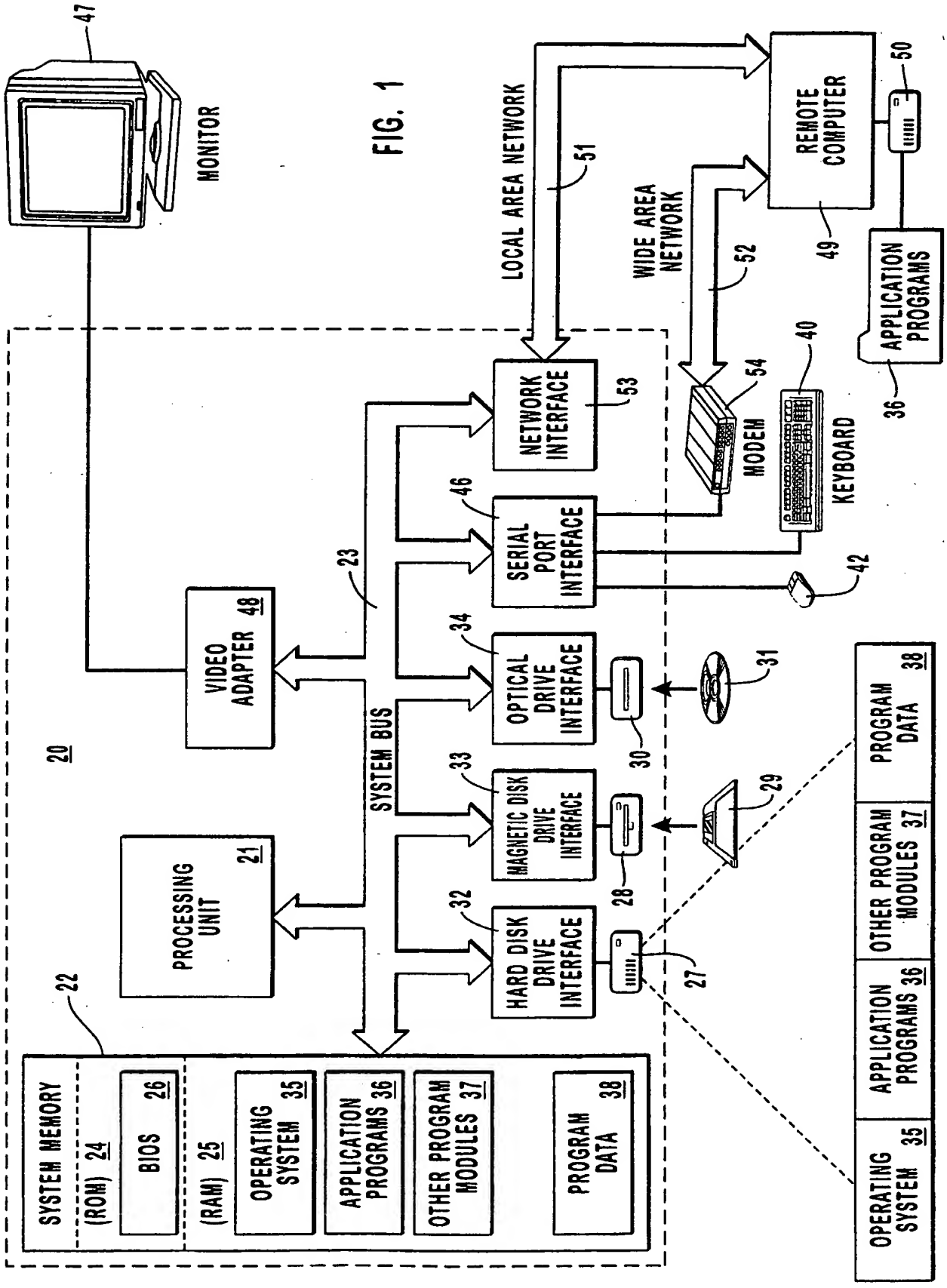
creating, at a packager, an object for those electronic messages associated with one or more policies; and

sending the object to a recipient specified by the sender.

35. A method as defined in claim 34, wherein the object comprises computer-executable code integrated with the electronic message, wherein the computer-executable code is representative of the one or more policies.

36. A method as defined in claim 34, wherein the object comprises coded instructions which reference computer-executable code stored in a remote location, wherein the coded instructions are representative of the one or more policies.

37. A method as defined in claim 34, wherein the step of creating an object further comprises the step of encrypting the electronic message.



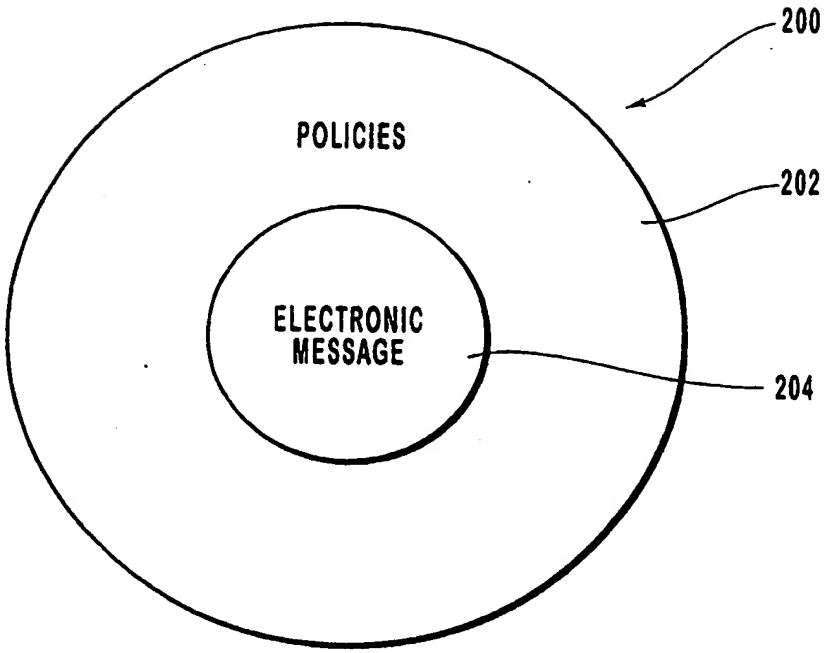


FIG. 2

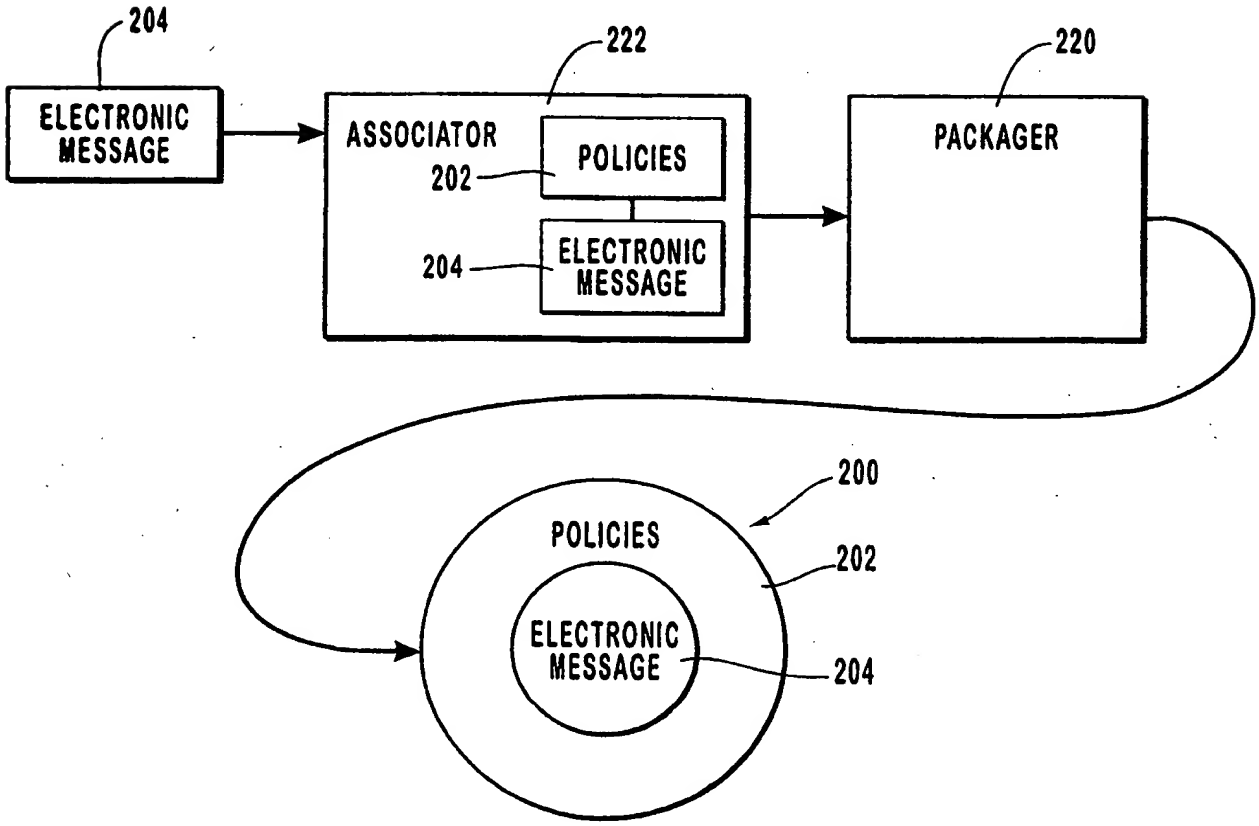


FIG. 3

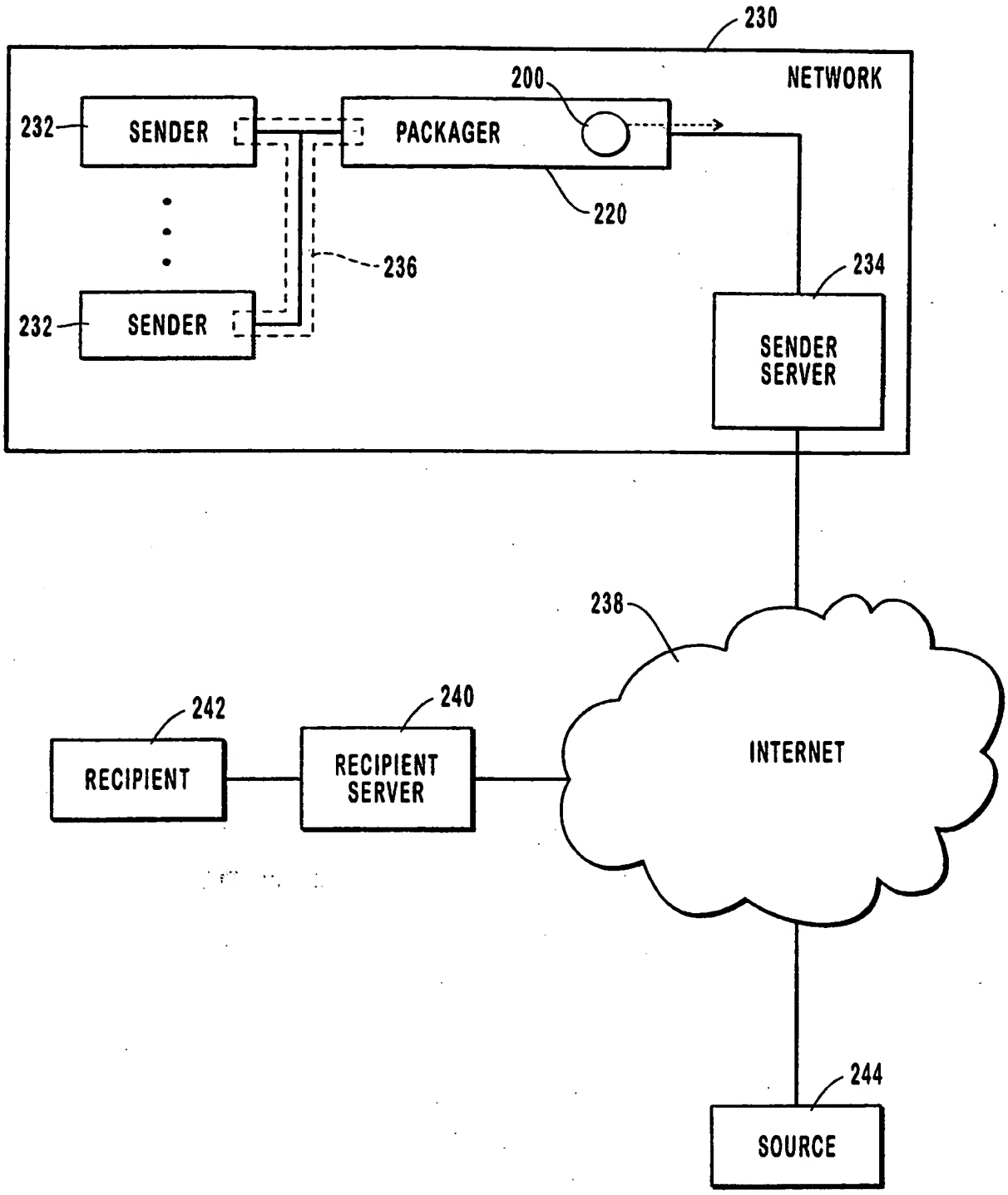


FIG. 4

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06K 17/00

A3

(11) International Publication Number: **WO 00/08794**

(43) International Publication Date: 17 February 2000 (17.02.00)

(21) International Application Number: PCT/US99/17786

(22) International Filing Date: 4 August 1999 (04.08.99)

(30) Priority Data:

09/129,467	4 August 1998 (04.08.98)	US
Not furnished	4 August 1999 (04.08.99)	US

(71)(72) Applicants and Inventors: SENATOR, Steven, T. [US/US]; 8625 Westminster Drive, Colorado Springs, CO 89020 (US). BLUMENTHAL, John [US/US]; 4432 East Emigration Canyon, Salt Lake City, UT 84018 (US). MULLIGAN, M., Geoff [US/US]; 2175 Cloverdale Drive, Colorado Springs, CO 80920 (US). FRASCADORE, Gregory, A. [US/US]; 9505 Morgan Road, Colorado Springs, CO 80908 (US).

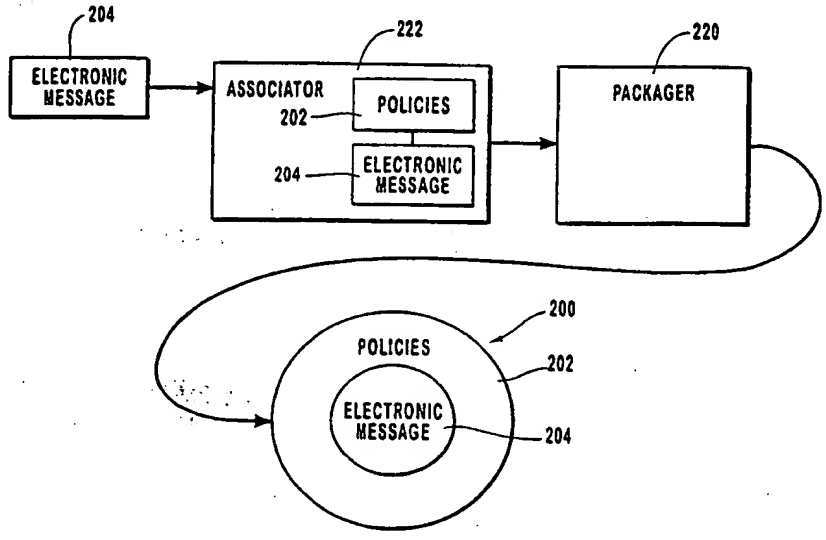
(74) Agents: STRINGHAM, John, C. et al.; Workman, Nydegger & Seeley, 1000 Eagle Gate Tower, 60 East South Temple, Salt Lake City, UT 84111 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(88) Date of publication of the international search report:
18 May 2000 (18.05.00)

(54) Title: SYSTEMS AND METHODS FOR SECURING ELECTRONIC MESSAGE



(57) Abstract

System and methods are provided for permitting a sender to control access to an electronic message. The sender selects one or more policies (202) which are packaged (220) with the electronic message (204) to form an object (222). The policies are implemented as computer-executable instructions capable of execution on a remote computer. The recipient can only access the electronic message as dictated by the policies which are in the object. Unauthorized use of the electronic message is substantially prevented and the electronic message remains in the control of the sender.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

INTERNATIONAL SEARCH REPORT

Inte .ional application No.
PCT/US99/17786

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :GO6K 17/00
US CL :709/206

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 709/206

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

west.stn

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,325,310 A (JOHNSON ET AL) 28 JUNE 1994, ABSTRACT, COL. 25-32, AND COL. 8, 46-51).	1-4,6-14, 16-27, 30-36
X,P	US 5,903,652 A (MITAL) 11 MAY 1999, ALL	5,15,28,29
A	US 5,786,817 A (SAKANO ET AL) 28 JULY 1998, ALL	1-37
A,P	US 5,893,910 A (MARTINEAU ET AL) 13 APRIL 1999, ALL	1-37
A,E	US 5,937,161 A (MULLIGAN ET AL) 10 AUGUST 1999, ALL	1-37

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 FEBRUARY 2000	23 FEB 2000

Name and mailing address of the ISA/US	Authorized officer
Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	GLENTON BURGESS FOR Regina Fogner
Facsimile No. (703) 305-3230	Telephone No. (703) 305-4792

Form PCT/ISA/210 (second sheet)(July 1992)★